Autenticazione digitale

Andrea Mattasoglio
CILEA, Segrate

Abstract
Questo articolo presenta una breve introduzione al tema dell'autenticazione digitale e un insieme di articoli che descrivono architetture e tecniche implementate o progettate al CILEA per l'autenticazione.

I introduce the topic of digital authentication and a set of articles describing architectures and techniques for authentication implemented or designed by CILEA.

Keywords: Computer Networks, Distributed Application, Authentication.

Nella realizzazione di sistemi informativi distribuiti sicuri sorge spesso l'esigenza di verificare che il proprio interlocutore sia effettivamente chi dichiara di essere. Questo tipicamente avviene perché dall'autenticazione discende, qualche volta implicitamente, l'autorizzazione a utilizzare un servizio richiesto o a svolgere una determinata azione.

I metodi tramite i quali si può autenticare una persona, un utente, sono divisi in tre classi, in base a ciò che:

- **è:** per esempio impronte digitali [1], impronta vocale [2], modello retinico, sequenza del DNA [3], calligrafia [4] o altri identificatori bio_metrici;
- **ha:** tesserino identificativo, certificato;
- **conosce:** password, parola chiave o numero di identificazione personale (PIN [5]).

Per l'autenticazione in rete viene normalmente usata la terza classe, che non richiede né l'utilizzo di hardware speciali né la presenza dell'utente.

Per ragioni di sicurezza, la password scelta dall'utente, o a lui assegnata, deve soddisfare certe requisiti ed essere:

- non ovvia e di lunghezza minima data (non attaccabile con metodi *brute force* o basati sulla *social engineering*);
- non comunicata in chiaro;
- cambiata con una certa frequenza.

Per soddisfare il primo requisito, una password deve essere complicata e possibilmente contenere anche numeri e segni di punteggiatura. Considerando che la password deve anche essere cambiata spesso, ne discende che per l'utente può diventare gravoso ricordare una coppia username/password. Ancora di più se poi deve ricordare le due stringhe e i loro cambiamenti nel tempo per ciascun servizio che usa. Per questo motivo, recentemente si tende a sviluppare sistemi di autenticazione che possano essere riutilizzabili per varie funzioni, o servizi. In alcuni casi, tali sistemi si occupano di gestire un'unica coppia username/password associata a un utente, che deve comunque fornirla per ciascun servizio che intende utilizzare. In altri casi, almeno per quanto riguarda servizi diversi accessibili all'interno di un'unica università/azienda, esistono dei veri e propri sistemi di Single Sign On, in cui un utente si autentica una volta soltanto e accede poi liberamente a tutti i servizi per cui possiede l'autorizzazione. Di tali sistemi ne esistono ormai vari e la scelta non è sempre facile e spesso dipende da molte variabili. Proprio per questo il CILEA sta sperimentando tre diverse soluzioni integrate per tre ambienti applicativi distinti, presentate in altrettanti articoli di questo bollettino.

Nel primo degli articoli, "Una soluzione LDAP per il Single Sign On", si descrive il meccanismo implementato per l'autenticazione delle funzioni di automazione di ufficio dei dipendenti CILEA. Esso si basa sul protocollo

LDAP ed è particolarmente adatto a questa funzione, perché la sua base di utenti è abbastanza stabile e quindi non viene aggiornato molto frequentemente. LDAP infatti è più efficiente nelle funzioni di lettura che in quelle di aggiornamento.

Nel secondo articolo, "Singl Sign On per applicazioni Web", viene descritta l'architettura di autenticazione utilizzata per il sistema informativo SIRIO, nel quale le funzioni di autenticazioni sono inserite nel database, che offre ottime prestazioni sia in lettura che in aggiornamento. Tale scelta è coerente con il tipo di utenza di SIRIO, che utilizza il sistema per presentare domande di finanziamento su bandi ed è quindi soggetta a frequenti cambiamenti.

Nel terzo articolo, "L'autenticazione in GRID", viene descritta l'articolazione dell'autenticazione distribuita del sistema GRID, utilizzato per compiere calcoli su calcolatori di qualsiasi organizzazione partecipi alla griglia computazionale.

Due ulteriori articoli trattano invece l'argomento della creazione di federazioni di istituzioni e organizzazioni che condividano in dati di autenticazione dei propri utenti. Il primo articolo, "Il CILEA collabora alla creazione della federazione AAI italiana", descrive un'iniziativa del GARR, che vede il CILEA protagonista. Il progetto prevede la creazione di una federazione italiana di infrastrutture di autenticazione e autorizzazione, di cui il CILEA deve diventare un *service provider*. Un secondo articolo, "AAI: Autenticazione federata e biblioteche digitali", descrive come il problema dell'autenticazione federata sia al momento recepito da parte degli editori di contenuti in formato digitale.

Bibliografia

[1] URL: http://it.wikipedia.org/wiki/Impronta_digitale
[2] URL: http://it.wikipedia.org/wiki/Impronta_vocale
[3] URL: http://it.wikipedia.org/wiki/DNA
[4] URL: http://it.wikipedia.org/wiki/Calligrafia
[5] URL: http://it.wikipedia.org/wiki/PIN